REMARKS

The present amendment is submitted in an earnest effort to advance this case to issue without delay.

1. Claims land 8, the independent claims in the case have been amended to define the invention more sharply over the references as combined by the Examiner. In particular, the amendments make clear that each of the providers has a specific enabling algorithm which is selectively loaded into the smart card, i.e. the single removable user unit for enabling the use of the specific provider.

2. The claims have been rejected under 35 USC 103 as being obvious from Wasilewski in view of Jardin. Applicants have reviewed the rejection in depth and have discussed it below. However, at this point, Applicants wish to observe that the Examiner has recognized that Wasilewski does not expressly disclose incorporating a respective enabling algorithm associated with a particular provider selectively into the smart card. While Jardin may disclose downloading an algorithm to a client application it also does not expressly disclose incorporating an algorithm of a

provider into a smart card. Indeed, what the invention does is diametrically oppose to what Wasilewski discloses and in the sense that Jardin does not have a particular algorithm for each of a number of providers but rather a pool of algorithms, is aditionally opposite what Jardin does.

The combination of the two would not yield the claimed invention except if one ignored the pool of Jardin and the alternative method of coding the smart card in Wasilewski. Thus, the obvious combination of these reference does not meet either claim 1 or 8. Furthermore, the combination would not have been obvious at the time the invention was made from either reference in accordance with the principles of (Ashland Oil Inc. V. Delta Resin & Refractories, Inc., 227 USPQ 657). There it is made clear that the combination must derive from a teaching specific to at least one of the references and may not have a deduction made by the Examiner from Applicants' own disclosure.

3. Applicants believe that reconsideration of the rejection is in order for the following reasons:

The Examiner has rejected claims 1-3, 5-6, 8-10, and 12-13 under 35

U.S.C. 103(a) as being unpatentable over Wasilewski et al (6,157,719) in view of Jardin (6,671,810). Wasilewski discloses, inter alia, a conditional access system wherein a Set Top Box (DHCT-333) comprises a DHCT secure element (DHCTSE-627) for performing security and conditional access-related functions (Wasilewski, Col.15, 1.35-43).

The DHCTSE 627 may be an integral part of DHCT 333 or it may be contained in a user-installable module such as a "smart-card" (Wasilewski, Col.21, 1.11-13).

Memory 1207 [of DHCTSE 627] contains the code executed by microprocessor 1201, the keys, and the entitlement information (Wasilewski, Col.21, 1.28-29).

Memory 1207 in DHCTSE ... (Omissis) is divided in two main parts: [first part] read-only storage 1301, ... (Omissis) Ro storage 1301 contains code 1305.

Code 1305 falls into four categories: code 1307 for the encryption, decryption, and authentication operations performed by DHCTSE 627 (Wasilewski, Col.21, 1.47-56)-Memory 1207 in DHCTSE ... (Omissis) is divided in two main parts: and [second part] NVA storage 1303, which is non-volatile storage that changes as a result of the interpretation of EMMs (Wasilewski, Col.21, 1.47-53). NVA storage 1303 has ...(Omissis) administrative storage 1330 and EA [Entitlement Agent] storage 1331. Administrative storage 1330 contains DHCT Keys 1325, CAA [Conditional Access Authority] Keys 1329 and CAA data 1330 (Wasilewski, Col.22, 1.9-12).

The amount of memory 1207 in DHCTSE is limited. The CAA manages this scarce resource and allocates it to the Entitlement Agents from which DHCT 333 receives services (Wasilewski, Col.23, 1.49-51).

Any one of the public keys for a CAA can be replaced by means of a sequence of two EMM, (Wasilewski, Col.25, 1.4-5).

In summary, Wasilewski teaches, inter alia, a conditional access system comprising a Set Top Box or STB (DHCT) having one Smart Card (DHCTSE) for providing to a user services by a plurality of Entitlement Agents.

The Smart card comprises a single NOT MODIFIABLE algorithm stored therein and a plurality of MODIFIABLE keys.

The single NOT MODIFIABLE algorithm is THE SAME for ALL THE ENTITLEMENT AGENTS.

The STB through the single NOT MODIFIABLE algorithm and the plurality of MODIFIABLE keys is able to provide services to a plurality of Entitlement Agents (Service Providers).

In other words, according to the Wasilewski teaching, all the Service Providers use the same encryption/decryption algorithm and different keys, stored in the Smart Card.

Jardin discloses, inter alia, a method and system to provide secure communication over a network. A server on the network responds to an initiating event by randomly selecting a cryptographic algorithm ...(Omissis) and then downloads the selected algorithm ... (Omissis) to the requesting application program (Jardin, Abstract).

In summary, Jardin discloses a method and system wherein a single server is able to selectively download one algorithm to a requesting application or, in other words, a method and system wherein the single server may selectively replace the downloaded algorithm.

Applicant respectfully objects to the Examiner that by applying the teaching of Jardin to the teaching of Wasilewski it could be possible to replace the single NOT MODIFIABLE algorithm of Wasilewski with the selectable algorithm of Jardin, BUT it could not be possible to the Entitlement Agents to use different or respective algorithms.

In other words, by applying the teaching of Jardin to the Wasilewski teaching, all the Service Providers could use the same set of encryption/decryption algorithms to be selectively stored and different keys.

No teaching is present in Wasilewski nor in Jardin applied to Wasilewski regarding the possibility that each Entitlement Agent (Service Provider) may use different or respective algorithms.

In fact, Wasilewski suggest the use of one algorithm usable by all the service providers.

Jardin suggests a centralized server able to select and download one algorithm in a set.

The teaching of downloading different or respective algorithms by each service provider is, in the Applicant view, one of the main features of present invention as disclosed and now clearly claimed.

Such a feature is clearly disclosed, for example, at Page 5, 1.16-19:

"In the solution according to the invention the smart card 105, in addition to containing a cryptographic key that is not modifiable or legible from the outside, is able to receive, verify, store and execute an algorithm that allows using the services delivered by a given provider." Applicant respectfully notes that the solution according to present invention is exactly the opposite of the Wasilewski teaching.

at Page 7, 1.18-22 of the disclosure:

"In use, when the user U chooses a particular provider SP (this can be done through a normal selection operation effected by acting on a remote control set) a so-called applet generated by the provider SP is transferred through the system STB for being loaded into the respective unit 105. As is well known, the term "applet indicates a set of Java instructions that implements a given algorithm."

Claims 1 and 8 are thus allowable with the claims that depend therefrom.

4. The Examiner has also rejected claims on this combination and Jones Patent 5,623,637. It is the Examiner's

position that the host in the Jones system provides a trusted middleware function in the smart card.

Col. 2, lines 23 through 29 of Jones is directed to removable memory cards conforming to the PCM CIA in face standard, i.e. a standard plug in memory card rather than a smart card or anything of the sort. The Examiner has not explained why the ordinary skilled worker in the art would associated Jones with a smart card application and here again has failed to make a prima facie case of the obviousness of the rejected claims (4 and 11).

It would appear, therefore, that the independent claims, the claims dependent therefrom and especially claims 4 to 11, all ought to be considered to be allowable over the references and an early notice to that affect is earnestly solicited.

Respectfully submitted,
The Firm of Karl F. Ross P.C.

Herbert Dubno, Reg. No. 19,752
Attorney for Applicant

db-
DATED: August 9, 2004
5676 Riverdale Avenue Box 900
Bronx, NY 10471-0900
Cust. No.: 535
Tel: (718) 884-6600
Fax: (718) 601-1099